JOURNAL OF COMBINATORIAL THEORY (A) 18, 313–335 (1975)

On the Classification and Enumeration of Self-Dual Codes

VERA PLESS*

Project MAC, MIT, Cambridge, Massachusetts 02138

AND

N. J. A. SLOANE

Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by the Managing Editors

Received December 17, 1973

A complete classification is given of all [22, 11] and [24, 12] binary self-dual codes. For each code we give the order of its group, the number of codes equivalent to it, and its weight distribution. There is a unique [24, 12, 6] self-dual code. Several theorems on the enumeration of self-dual codes are used, including formulas for the number of such codes with minimum distance $\geqslant 4$, and for the sum of the weight enumerators of all such codes of length n. Self-orthogonal codes which are generated by code words of weight 4 are completely characterized.

1. INTRODUCTION

In spite of 25 years of research [2, 31], even the codes of only moderate length, up to 50 say, are a long way from being understood. Slepian [38] used Pólya's counting theorem to find the number of inequivalent codes of length n and dimension k. But as he pointed out the classification by length, dimension, and minimum distance is much more difficult. Self-dual codes ($C = C^{\perp}$) are an important subclass of codes, both for practical purposes (many of the best codes known are of this type), and theoretically, in view of their connections with block designs, geometric lattices, and

* The work of the first author was supported in part by Project MAC, and MIT interdepartmental laboratory sponsored by the Advanced Research Projects Agency, Department of Defense, under Office of Naval Research Contract N00014-70-A-0362-0001.

simple groups [1, 7–10, 22, 29]. Therefore there has been interest in the complete enumeration of short self-dual codes, in order to see what kinds of codes do exist, which weight distributions are possible, and which groups arise as automorphism groups of such codes. The first author in [34] has classified and enumerated all self-dual codes of length $n \leqslant 20$. In the present paper we extend this to lengths 22 and 24. For each indecomposable code we give the order of its group, the number of codes equivalent to it, and its weight distribution. (These codes provide 22- and 24-dimensional representations over $GF(2)$ of their groups.) Besides the well-known unique self-dual code of length 24 and minimum distance 8, we were surprised to find a unique code of minimum distance 6 (Z_{24} in Table II); its group is a maximal subgroup of the Mathieu group $\mathscr{M}_{24}$.

The numbers of inequivalent self-dual codes are as follows.

Length n	2	4	6	8	10	12	14	16	18	20	22	24
Indecomposable codes	1	0	0	1	0	1	1	2	2	6	8	26
All codes	1	1	1	2	2	3	4	7	9	16	25	55

If we require that the weights of code words be divisible by 4, then n must be a multiple of 8, and the corresponding numbers are

Length n	8	16	24
Indecomposable codes	1	1	7
All codes	1	2	9

The 9 codes of length 24 with weights divisible by 4 were first found by J. H. Conway (unpublished). Niemeier [29; see also 28] has found that there are 24 inequivalent even unimodular lattices in dimension 24, of which 9 correspond to these codes.

Some general results on the enumeration of self-dual codes have been given in [24, 32, 33, 35] (including a proof that these codes meet the Gilbert bound), but were inadequate for our purpose, and so in Sections 3–6 several new theorems are given (summarized in the abstract).

2. Terms from Coding Theory

For standard coding theory terms see [2, 31]. All codes are binary and linear. An $[n, k, d]$ (or $[n, k]$ for short) code has length n, dimension k, and (minimum) distance exactly d, and is a subspace of F^n, where

$F = \{0, 1\}$. $|u|$ denotes the weight of u, and $u \cap v = (u_1v_1, \ldots, u_nv_n)$. $C^\perp$ is the dual code to C. A code is *self-orthogonal* (s.o.) if $C \subset C^\perp$, it is *self-dual* if $C = C^\perp$. The *deficiency* of a s.o. code is $\delta = \frac{1}{2}n - k$. For a self-dual code, n is even, $\delta = 0$, and the weight of every code word is divisible by 2. It is possible, and interesting, to require that the weight of every code word be divisible by 4, in which case n must by a multiple of 8 (cf. Theorem 2.5). Note that if the basis vectors of a self-orthogonal code have weights divisible by 4, then all the code words have this property.

Three important self-dual codes are

(i) The [2, 1, 2] code $C_2 = \{00, 11\}$.

(ii) The [8, 4, 4] Hamming code E_8, which is spanned by the rows of its generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & 1 & & \\ & & & & 1 & 1 & 1 & 1 \\ 1 & & 1 & & 1 & & 1 & \end{pmatrix}. \tag{2.1}$$

(Blanks denote zeros.)

(iii) The [24, 12, 8] Golay code G_{24}, with generator matrix given by (2.2) [9].

G_{24}:

$$\left[\begin{array}{cccccccccccc|c} 1 & & & & & & & & & & & & 1 \\ & 1 & & & & & & & & & & & 1 \\ & & 1 & & & & & & & & & & 1 \\ & & & 1 & & & & & & & & & 1 \\ & & & & 1 & & & & & & & & 1 \\ & & & & & 1 & & & & & & & 1 \\ & & & & & & 1 & & & & & & 1 \\ & & & & & & & 1 & & & & & 1 \\ & & & & & & & & 1 & & & & 1 \\ & & & & & & & & & 1 & & & 1 \\ & & & & & & & & & & 1 & & 1 \\ & & & & & & & & & & & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \end{array}\right.\quad \left.\begin{array}{c|c} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ \hline & \end{array}\right] \tag{2.2}$$

The *group* $\mathcal{G}(C)$ of C consists of all permutations of the coordinates which send code words into code words (i.e. fix C setwise). $\mathcal{G}(C)$ is a subgroup of the symmetric group $\mathcal{S}_n$. E.g. $\mathcal{G}(C_2)$ is $\mathcal{Z}_2$, the cyclic group of order 2; $\mathcal{G}(E_8)$ is the general affine group $\mathcal{GA}_3(2)$ of order 1344 (all transformations $\mathbf{x} \to \mathbf{x}A + \mathbf{b}$ where A is an invertible 3×3 matrix); and $\mathcal{G}(G_{24})$ is the Mathieu group $\mathcal{M}_{24}$ of order $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$.

There is an extensive literature on G_{24}, $\mathscr{M}_{24}$, and the associated Steiner system and Leech lattice; see Refs. [1, 3, 7–10, 15, 16, 19, 21, 22, 30, 33, 39, 40, 42, 43].

Two codes C, C' are *equivalent* if there exists a permutation in $\mathscr{S}_n$ sending C into C'. The size of the equivalence class containing C is $n!$/order of $\mathscr{G}(C)$.

The *direct sum* of codes $C[n, k, d]$ and $C'[n', k', d']$ is the $[n + n', k + k', \min(d, d')]$ code $C \oplus C' = \{(u_1 \cdots u_n v_1 \cdots v_n)\colon (u_1 \cdots u_n) \in C, (v_1 \cdots v_n) \in C'\}$. $C \oplus C$ will be written $2C$, etc. If D can be written $C \oplus C'$ it is called *decomposable*, otherwise *indecomposable* [38].

If $\mathscr{G}$, $\mathscr{H}$ are groups we write $\mathscr{G} \times \mathscr{H}$ for their direct product, $\mathscr{G}^k$ for $\mathscr{G} \times \cdots \times \mathscr{G}$ (k factors), and $\mathscr{G} \cdot \mathscr{H}$ for a semidirect product.

LEMMA 2.3. *If $C = C_1 \oplus \cdots \oplus C_k$ where the C_i are indecomposable and equivalent then $\mathscr{G}(C) = \mathscr{G}(C_i)^k \cdot \mathscr{S}_k$.*

LEMMA 2.4. *Let $C = D_1 \oplus \cdots \oplus D_l$ where each D_i is a direct sum of equivalent codes, and for $i \neq j$ no summand of D_i is equivalent to a summand of D_j. Then*

$$\mathscr{G}(C) = \prod_{i=1}^{l} \mathscr{G}(D_i).$$

Consider the family of self-orthogonal codes with minimum distance $\geqslant d$ and having all weights divisible by w. Then the number of indecomposable codes and the total number (decomposable or indecomposable) are related by exactly the same Riddell–Gilbert formula [6; 11; 12; 36, p. 147] which relates the numbers of connected graphs and all graphs.

The *weight distribution* of C consists of the numbers $\alpha_0, \ldots, \alpha_n$ where α_i is the number of code words of weight i. The *weight enumerator* of C is the polynomial

$$\omega(C) = \omega(C; x) = \sum_{i=0}^{n} \alpha_i x^i.$$

For example,

$$\omega(C_2) = 1 + x^2, \qquad \omega(E_8) = 1 + 14x^4 + x^8.$$

THEOREM 2.5 (Gleason [13]; see also [4, 14, 23, 25].). (a) *The weight enumerator of a self-dual code is a polynomial in $\omega(C_2)$ and $\omega(E_8)$.* (b) *If in addition the weight of every code word is a multiple of 4, then the weight enumerator is a polynomial in $\omega(E_8)$ and $\omega(G_{24})$.*

Notation. Usually capital Latin letters (A_{24},...) denote codes, the subscript giving the length. d_n, e_n are special codes, and $a = 101010\cdots10$, $b = 110000\cdots00$, $a' = a + b = 011010\cdots10$, $c = \mathbf{1} = 111\cdots1$ are special vectors. Also $y_{22} = 1\cdot3\cdot5\cdot7\cdot\cdots\cdot19\cdot21 = 13{,}749{,}310{,}575$ and $y_{24} = 1\cdot3\cdot5\cdot7\cdot\cdots\cdot21\cdot23 = 316{,}234{,}143{,}225$.

3. General Enumeration Theorems

Define, for $0 \leqslant k \leqslant n/2$

$\Phi_{n,k}$ = the class of self-orthogonal $[n, k]$ codes,

$\Phi'_{n,k}$ = subclass of $\Phi_{n,k}$ of codes which contain $\mathbf{1}$,

$\Psi_{n,k}$ = subclass of $\Phi_{n,k}$ of codes in which every code word has weight divisible by 4,

$\Psi'_{n,k}$ = subclass of $\Psi_{n,k}$ of codes which contain $\mathbf{1}$.

Then $\Phi_{n,n/2} = \Phi'_{n,n/2}$ is the class of self-dual codes of length n. The following results are useful for enumerating self-dual codes. Some of these results appeared in [24, 32, 33]. They are all proved by the methods of [24, 32], i.e. by induction on k. An empty product is equal to 1.

THEOREM 3.1. *Let n be even and $C \in \Phi'_{n,s}$. The number of codes in $\Phi'_{n,k} (k \geqslant s)$ which contain C is*

$$\prod_{j=0}^{k-s-1} \frac{2^{n-2s-2j} - 1}{2^{j+1} - 1}.$$

COROLLARY 3.2 [24]. *Let n be even and $C \in \Phi'_{n,s}$. The number of codes in $\Phi'_{n,n/2}$ which contain C is*

$$\prod_{j=1}^{(n/2)-s} (2^j + 1).$$

COROLLARY 3.3 [32]. *The total number of codes in $\Phi'_{n,n/2}$ is*

$$\prod_{j=1}^{(n/2)-1} (2^j + 1).$$

COROLLARY 3.4. *The total number of codes in $\Phi'_{n,k}$ is*

$$\prod_{j=1}^{k-1} \frac{2^{n-2j} - 1}{2^j - 1} \quad \text{if } n \text{ even}, \quad 0 \text{ if } n \text{ odd}.$$

THEOREM 3.5. *Let $C \in \Phi_{n,s} - \Phi'_{n,s}$. The number of codes in $\Phi_{n,k} - \Phi'_{n,k}$ $(k \geqslant s)$ which contain C is*

$$2^{k-s} \prod_{j=1}^{k-s} \frac{2^{n-2s-2j} - 1}{2^j - 1} \quad (n \text{ even}), \qquad \prod_{j=1}^{k-s} \frac{2^{n-2s-2j+1} - 1}{2^j - 1} \quad (n \text{ odd}).$$

COROLLARY 3.6. *The total number of codes in $\Phi_{n,k} - \Phi'_{n,k}$ is*

$$2^k \prod_{j=1}^{k} \frac{2^{n-2j} - 1}{2^j - 1} \quad (n \text{ even}), \qquad \prod_{j=1}^{k} \frac{2^{n-2j+1} - 1}{2^j - 1} \quad (n \text{ odd}).$$

COROLLARY 3.7. *Let n be even and $C \in \Phi_{n,s} - \Phi'_{n,s}$. The number of codes in $\Phi_{n,k}$ $(k > s)$ which contain C is*

$$(2^{n-k-s} - 1) \prod_{j=1}^{k-s-1} (2^{n-2s-2j} - 1) \Big/ \prod_{j=1}^{k-s} (2^j - 1).$$

COROLLARY 3.8 [32]. *If n is even, the total number of codes in $\Phi_{n,k}$ is*

$$(2^{n-k} - 1) \prod_{j=1}^{k-1} (2^{n-2j} - 1) \Big/ \prod_{j=1}^{k} (2^j - 1).$$

For codes with weights divisible by 4 we do not give as much detail.

THEOREM 3.9. *Let n be a multiple of 8, and $C \in \Psi'_{n,s}$. The number of codes in $\Phi'_{n,k} - \Psi'_{n,k}$ $(k > s)$ which contain C is*

$$(2^{n-s-k} - 2^{(n/2)-k}) \prod_{j=1}^{k-s-1} \frac{2^{n-2s-2j} - 1}{2^j - 1}.$$

COROLLARY 3.10. *Same hypothesis as Theorem 3.9. Then the number of codes in $\Psi'_{n,k}$ $(k > s)$ which contain C is*

$$(2^{(n/2)-s} - 1)(2^{(n/2)-k} + 1) \prod_{j=1}^{k-s-1} (2^{n-2s-2j} - 1) \Big/ \prod_{j=1}^{k-s} (2^j - 1).$$

COROLLARY 3.11 [24]. *Same hypothesis as Theorem 3.9. The number of codes in $\Psi'_{n,n/2}$ which contain C is*

$$\prod_{j=0}^{(n/2)-s-1} (2^j + 1).$$

COROLLARY 3.12 [24]. *If n is a multiple of 8, the total number of codes in $\Psi'_{n,n/2}$ is*

$$\prod_{j=0}^{(n/2)-2} (2^j + 1).$$

4. The Sum of All Weight Enumerators

From the results of Section 3 it follows easily that (a) the sum of the weight enumerators of all self-dual codes of length n is (for n even)

$$\prod_{j=1}^{(n/2)-2} (2^j + 1) \cdot \left[2^{(n/2)-1}(1 + x^n) + \sum_{2|i} \binom{n}{i} x^i\right];$$

and (b) the corresponding sum when the weights are divisible by 4 is (for n divisible by 8)

$$\prod_{j=0}^{(n/2)-3} (2^j + 1) \cdot \left[2^{(n/2)-2}(1 + x^n) + \sum_{4|i} \binom{n}{i} x^i\right].$$

5. Codes with Minimum Distance at Least 4

Let C be a s.o. code of length n with minimum distance 2. The first two lemmas are immediate.

Lemma 5.1. *C is decomposable if $n > 2$.*

Lemma 5.2. *All code words of weight 2 in C are nonzero on disjoint sets of coordinates.*

Theorem 5.3. *Let n be even. The number of self-dual codes with length n and minimum distance $\geqslant 4$ is*

$$\sum_{i=0}^{n/2} \frac{(-1)^i\, n!}{2^i i!\,(n-2i)!}\, a(n-2i),$$

where $a(n) = \prod_{j=1}^{(n-1)/2} (2^j + 1)$.

Proof. Let $c(n, i)$ be the number of self-dual codes of length n containing i code words of weight 2. From 3.3,

$$\sum_{i=0}^{n/2} c(n, i) = a(n).$$

From 5.1, 5.2,

$$c(n, i) = \frac{n!}{2^i i!\,(n-2i)!}\, c(n-2i, 0),$$

$$\sum_{i=0}^{n/2} \frac{n!}{2^i i!\,(n-2i)!}\, c(n-2i, 0) = a(n).$$

The coefficients on the left are those of the Hermite polynomial $H_n(-x)$ [20]. The desired result follows from the orthogonality of these polynomials.

6. Codes With Minimum Distance Exactly 4

For $n = 4, 6, 8, \ldots$ let d_n be the s.o. $[n, \frac{1}{2}n - 1]$ code with generator matrix

$$d_n: \begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & \\ & & & & \cdot & \cdot & \cdot & & & \\ & & & & & & 1 & 1 & 1 & 1 \end{bmatrix}.$$

d_n has deficiency 1, weight enumerator $\frac{1}{2}[(1 + x^2)^{n/2} + (1 - x^2)^{n/2}]$, and dual code

$$d_n^{\perp} = d_n \cup (a + d_n) \cup (b + d_n) \cup (a' + d_n), \tag{6.1}$$

where a, b, a' are defined in Section 2. The group of d_n is: $\mathcal{G}(d_4) = \mathcal{S}_4$, $\mathcal{G}(d_n) = \mathcal{Z}_2^{n/2} \cdot \mathcal{S}_{n/2}$ if $n > 4$ [34].

For $n = 7, 11, 15, \ldots$ let e_n be the s.o. $[n, \frac{1}{2}(n-1)]$ code with generator matrix

$$e_n: \begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & \\ & & & & \cdot & \cdot & \cdot & & & \\ & & & & 1 & 1 & 1 & 1 & & \\ & & & & & & 1 & 1 & 1 & 1 \\ 1 & & 1 & & 1 & & 1 & & 1 & \end{bmatrix}.$$

e_n has deficiency $\frac{1}{2}$, weight enumerator $\frac{1}{2}[(1 + x^2)^{(n-1)/2} + (1 - x^2)^{(n-1)/2}] + 2^{(n-3)/2}x^{(n+1)/2}$, and dual code

$$e_n^{\perp} = e_n \cup (c + e_n). \tag{6.2}$$

The group is: $\mathcal{G}(e_7) = \mathcal{GL}_3(2) \simeq \mathcal{PSL}_2(7)$, of order 168; $\mathcal{G}(e_n) = \mathcal{Z}_2^{(n-3)/2} \cdot \mathcal{S}_{(n-1)/2}$ if $n > 7$ [34].

For $n = 8, 12, 16, \ldots$ let E_n be the $[n, n/2]$ self-dual code $d_n \cup (a + d_n)$. For E_8 see (2.1). The weight enumerator is $\frac{1}{2}[(1 + x^2)^{n/2} + (1 - x^2)^{n/2}] + 2^{(n/2)-1}x^{n/2}$. The group is: $\mathcal{G}(E_8) = \mathcal{GO}_3(2)$, of order 1344; $\mathcal{G}(E_n) = \mathcal{Z}_2^{(n/2)-1} \cdot \mathcal{S}_{n/2}$ if $n > 8$ [34].

From (6.1), (6.2), and the fact that E_n is self-dual, we have

Lemma 6.3. *Any code word of $d_n^{\perp}$ is equal to one of* 0, a, b, *or* a' *(modulo d_n); any code word of $e_n^{\perp}$ is equal to* 0 *or* c *(modulo e_n); and any code word of $E_n^{\perp}$ is equal to* 0 *(modulo E_n).*

Corollary 6.4. *If C is a* s.o. *code containing E_n as a subcode, then C is decomposable.*

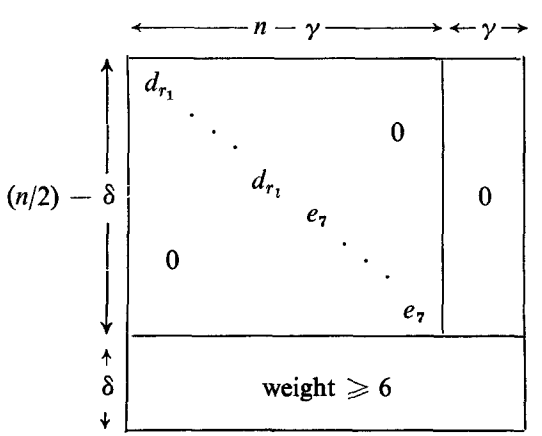
These codes are important because they provide a canonical form for codes generated by code words of weight 4, given in Theorem 6.5. This result is the basis of the classification in [34] and is used again in Sections 7, 8. The result was derived independently by J. H. Conway (unpublished).

THEOREM 6.5. *An indecomposable, self-orthogonal code C of length n which is generated by code words of weight* 4 *is either d_n ($n = 4, 6, 8, \ldots$), e_7, or E_8.*

Proof. Since C has a basis consisting of weight 4 vectors, there is a largest subspace C' of C whose basis is equivalent to a d_n. If $C = C'$, we are finished. If not, there is a code word x of weight 4 in C not in C'. Since x is orthogonal to C', the space generated by x and C' must either be e_7 or E_8. Now e_7 and E_8 are direct summands of any self-orthogonal code containing them, hence C is either e_7 or E_8.

COROLLARY 6.6. *The only self-dual codes which are generated by code words of weight* 4 *are $E_8 \oplus \cdots \oplus E_8$.*

Our notation for describing the generator matrix of an indecomposable self-dual code C with minimum distance equal to 4 is as follows. We take the maximum number of linearly independent code words of weight 4 as the top left-hand corner of the generator matrix. By 6.4, 6.5, this has the form $d_{r_1} \oplus \cdots \oplus d_{r_l} \oplus e_7 \oplus \cdots \oplus e_7$ (with m copies of e_7), or $d_{r_1} \cdots d_{r_l} e_7^m$ for short, for suitable $r_1, \ldots, r_l$, m. The generator matrix is



It is convenient to use the same symbol (d_r, e_7, etc.) for both

the code and its generator matrix. Here γ is called the *gap* of C, and $\delta = l + \frac{1}{2}m + \frac{1}{2}\gamma$ is the deficiency of the subcode generated by code words of weight 4. The last δ rows have weight $\geqslant 6$. If u is one of the last δ rows, by 6.3 we may assume that under each d_r, u is one of 0, a, b, or a', and under each e_7, u is either 0 or c.

To avoid writing the generator matrix in full we adopt a shorthand notation, best explained by an example. The code J_{24} of Section 8, with generator matrix given in (6.7)

J_{24}:

$$\left[\begin{array}{cccc|cccc|cccc|c}
1&1&1&1&&&&&&&&&&\\
&&1&1&1&1&&&&&&&&\\
&&&&1&1&1&1&&&&&&\\
\hline
&&&&&&&&1&1&1&1&&\\
&&&&&&&&&1&1&1&1&\\
&&&&1&&1&&&&&&&\\
\hline
&&&&&&&&1&1&1&1&&\\
&&&&&&&&&1&1&1&1&\\
&&&&1&&1&&&&&&&\\
\hline
1&1&&&&&&&1&1&1&1&1&\\
1&1&&&&&&&&&&&&1\\
1&&1&&1&&&&&&&&&1
\end{array}\right]$$

$$= \left[\begin{array}{c|c|c|c}
d_8 & 0 & 0 & 00\\
\hline
0 & e_7 & 0 & 00\\
\hline
0 & 0 & e_7 & 00\\
\hline
b & c & 0 & 10\\
\hline
b & 0 & c & 01\\
\hline
a & 0 & 0 & 11
\end{array}\right] \tag{6.7}$$

will be written $d_8e_7^2 + 2/bco10/boc01/ao^2 1^2$.

It seems difficult to find a formula for the number of self-dual codes of length n and minimum distance 4. However, the next theorem does provide a useful check on the enumeration of some of these codes.

For $n = 4m$, let Ω_n denote the class of self-dual codes of length n with the property that the code word **1** is the sum of m disjoint code words

of weight 4. For $C \in \Omega_n$ let $h(C)$ be the number of ways of writing $\mathbf{1}$ as a sum of m codewords of weight 4, and let

$$\theta_n = \sum_{C \in \Omega_n} h(C),$$

$$\varphi_n = \theta_n \Big/ \binom{n}{4}\binom{n-4}{4} \cdots \binom{4}{4}.$$

THEOREM 6.8. *An explicit formula for* φ_n *is*

$$\varphi_n = \sum_{i=0}^{m} (-3)^{m-i} \binom{m}{i} \psi_i ,$$

where

$$\psi_0 = 1, \qquad \psi_i = \prod_{j=1}^{i} (2^j + 1).$$

Proof. By Corollary 3.2, the total number of self-dual codes containing m disjoint code words of weight 4 is $\psi_m = \prod_{j=1}^{m} (2^j + 1)$. Classifying these codes according to the number, $2i$ say, of code words of weight 2, we find

$$\psi_m = \sum_{i=0}^{m} 3^i \binom{m}{i} \varphi_{n-4i} , \qquad \text{with} \quad \varphi_0 = 1.$$

Inversion of this recurrence (cf. [36, p. 49]) gives the desired result.

To calculate $h(C)$, it is sufficient to look at the subcode of C generated by code words of weight 4. It is easily seen that

$$h(d_n) = \begin{cases} (\frac{1}{2}n - 1)(\frac{1}{2}n - 3) \cdots 5 \cdot 3 \cdot 1 & \text{if } 4 \mid n, \\ 0 & \text{otherwise,} \end{cases}$$

$$h(e_7) = 0, \qquad h(E_8) = 7,$$

$$h(d_{r_1} \oplus d_{r_2} \oplus \cdots) = h(d_{r_1})\, h(d_{r_2}) \cdots .$$

As an example of Theorem 6.8, for $n = 8$ there is one code E_8 in Ω_8, the number of codes equivalent to E_8 is 30 [34], and so $\theta_8 = 7 \cdot 30$, $\varphi_8 = 6$.

7. Self-Dual Codes of Length 22

Theorem 7.1. *There are* 25 *inequivalent self-dual codes of length* 22, 17 *of which are decomposable and* 8 *indecomposable* (see Table I).

TABLE I

Indecomposable Self-dual Codes of Length 22

Code	Generator matrix / Order of group	Number of codes divided by y_{22}	Weight distribution α_2	α_4	α_6	α_8	α_{10}
G_{22}	Shortened Golay code $2^8 3^2 5 \cdot 7 \cdot 11$	92,160	0	0	77	330	616
N_{22}	$d_{14}e_7 + 1/bc1/ao1$ $2^6 \cdot 7!168$	$1{,}508\frac{4}{7}$	0	28	49	246	700
P_{22}	$d_{10}^2 + 2/b^2 1^2/ao01/oa10$ $(2^4 \cdot 5!)^2 \cdot 2$	11,088	0	20	57	270	676
Q_{22}	$d_6^3 d_{10}/b^3/a^2o/a'oa$ $(2^2 \cdot 3!)^2 \cdot 2^4 \cdot 5! \cdot 2$	36,960	0	16	61	282	664
R_{22}	$d_6 d_8 e_7 + 1/boc1/abo1/bao0$ $2^2 \cdot 3! \cdot 2^3 \cdot 4! \cdot 168$	105,600	0	16	61	282	664
S_{22}	$d_6^3 d_8 + 2/aob10/o^2a1^2/$ b^2o1^2/a^2o1^2 $(2^2 \cdot 3!)^2 2^3 \cdot 4! \cdot 2$	369,600	0	12	65	294	652
T_{22}	$d_4^2 d_6^2 + 2/aa'bo00/oaao10/$ $aa'ob1^2/oa'oa10/b^2o^21^2$ $4^2 \cdot (2^2 \cdot 3!)^2 \cdot 2 \cdot 2$	2,217,600	0	8	69	306	640
U_{22}	$d_4^4 + 6/\ldots$ (see (7.2)) $4^4 \cdot 4! \cdot 6$	2,217,600	0	4	73	318	628
	Total	$6{,}241{,}559\frac{34}{49} \cdot y_{22}$					

The proof is similar to that of Theorem 8.1 and is omitted. Note that G_{22} is obtained from the Golay code G_{24} by using the code words beginning 00 or 11; its group is twice the Mathieu group $\mathcal{M}_{22}$.

U_{22} has generator matrix enclosed by the double line in (7.2).

U_{22} and Z_{24}:

$$
\left[\begin{array}{cccc|cccc|cccc|cccc|cccccc||c}
1&1&1&1&&&&&&&&&&&&&&&&&&&&&&1&1\\
&&&&1&1&1&1&&&&&&&&&&&&&&&&&&1&1\\
&&&&&&&&1&1&1&1&&&&&&&&&&&&&&1&1\\
&&&&&&&&&&&&1&1&1&1&&&&&&&&&&1&1\\
&&&&&&&&&&&&&&&&1&1&1&1&1&1&&&1&1\\
\hline
1&1&&&&&&&1&1&&&1&1&&&&&&&&&&&&\\
1&&1&&&&&&1&&1&&&&1&1&&&&&&&&&&\\
\hline
&&&&1&1&&&1&1&&&&&&&1&&1&&&&&&&&\\
&&&&1&&1&&1&&1&&1&&&&&&&1&&&&&&&\\
\hline
&&&&&&&&&&&&&&&&&&&&1&1&&&&\\
&&&&&&&&&&&&&&&&&&&&1&&1&&&\\
\hline
&&&&1&1&&&1&1&&&&&&&&&&&&&&&&\\
&&&&1&&1&&1&&1&&&&&&&&&&&&&&&&\\
\hline
&&&&&&&&&&&&&&&&&&&&&&&&&\\
\hline
&&&1&&&1&&&&&1&1&&&&&&&&&&&&&1
\end{array}\right] \qquad (7.2)
$$

8. Self-Dual Codes of Length 24

THEOREM 8.1. *There are* 55 *inequivalent self-dual codes of length* 24, 29 *of which are decomposable and* 26 *indecomposable* (Table II).

Proof. The decomposable codes and their groups are obtained immediately from [34], Table I, and Lemmas 2.3 and 2.4. The indecomposable codes are then classified according to their minimum distance which, by 5.1, is $\geqslant 4$. It is known [33, 39] that the Golay code G_{24} is the unique code of length 24 and distance 8.

Now suppose C is an indecomposable self-dual code of length 24 and distance 4, and let

$$C' = d_{r_1} \oplus \cdots \oplus d_{r_l} \oplus e_7 \oplus \cdots \oplus e_7 = d_{r_1} \cdots d_{r_l} e_7^m \qquad (8.2)$$

be the maximal subcode generated by code words of weight 4 (Section 6). C' has gap $\gamma = 24 - r_1 - \cdots - r_l - 7m$, and deficiency $\delta = l + \frac{1}{2}m + \frac{1}{2}\gamma$.

Our method is to consider each possible form (8.2) for C', and to find all ways of adding δ linearly independent generators to C' so as to obtain an indecomposable self-dual code C of distance 4. We call such a code C (indecomposable, self-dual, minimum distance 4, and with all code

TABLE II

Indecomposable Self-Dual Codes of Length 24

Code	Generator matrix / Order of group	Number of codes $\div y_{24}$	Weight distribution α_4	α_6	α_8	α_{10}	α_{12}
A_{24}	* $d_{12}^2/ab/ba$ $(2^5 \cdot 6!)^2 \cdot 2$	1,848	30	0	639	0	2756
B_{24}	* $d_{10}e_7^2/bcc/aoc$ $2^4 \cdot 5!168^2 \cdot 2$	$18{,}102\frac{6}{7}$	24	0	663	0	2720
C_{24}	* $d_8^3(a)/abb/bab/bba$ $(2^3 \cdot 4!)^3 \cdot 3!$	46,200	18	0	687	0	2684
D_{24}	* $d_6^4(a)/baao/obaa/aoba/aaob$ $(2^2 \cdot 3!)^4 4!$	246,400	12	0	711	0	2648
E_{24}	* d_{24}/a $2^{11} \cdot 12$	2	66	0	495	0	2972
F_{24}	* $d_4^6(a)/boa^3o/oboa^3/aoboa^2/$ $a^2oboa/a^3obo/oa^3ob$ $4^6 \cdot 6!3$	221,760	6	0	735	0	2612
G_{24}	* Golay code (see (2.2)) $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$8{,}013\frac{21}{23}$	0	0	759	0	2576
H_{24}	$d_8d_{16}/ab/ba$ $2^3 \cdot 4!2^7 \cdot 8!$	1,980	34	64	239	960	1500
I_{24}	$d_4d_8d_{12}/b^3/a^2o/oa^2$ $2 \cdot 2!2^3 \cdot 4!2^5 \cdot 6!$	110,880	22	64	287	960	1428
J_{24}	$d_8e_7^2 + 2/bco10/boc01/$ ao^21^2 (see (6.7)) $2^3 \cdot 4!168^2 \cdot 2$	$181{,}028\frac{4}{7}$	20	64	295	960	1416
K_{24}	$d_6d_{10}e_7 + 1/b^2c1/oao1/abo1$ $2^2 \cdot 3!2^4 \cdot 5!168$	253,440	20	64	295	960	1416
L_{24}	$d_8^3(b)/b^3/a^2o/oa^2$ $(2^3 \cdot 4!)^3 \cdot 3!$	46,200	18	64	303	960	1404
M_{24}	$d_8^3(c)/a^3/ba'o/boa'$ $(2^3 \cdot 4!)^3 \cdot 2$	138,600	18	64	303	960	1404

* Subtotal with weights divisible by 4: $542{,}744\frac{362}{1127} \cdot y_{24}$; total: $556{,}041{,}557\frac{86}{1127} \cdot y_{24}$.

Table continued

TABLE II (*continued*)

Code	Generator matrix / Order of group	Number of codes $\div y_{24}$	Weight distribution α_4	α_6	α_8	α_{10}	α_{12}
N_{24}	$d_6^2d_{10} + 2/b^311/oa^211/abo01/bao10$ $(2^2 \cdot 3!)^2 2^4 \cdot 5!2$	887,040	16	64	311	960	1392
O_{24}	$d_4^2d_8^2/ab^2o/boao/oboa/baob$ $(2 \cdot 2!)^2(2^3 \cdot 4!)^2 \cdot 2$	1,663,200	14	64	319	960	1380
P_{24}	$d_4d_6^2e_7 + 1/ob^2c1/ab^2o0/oaa'o0/boao1$ $2 \cdot 2!(2^2 \cdot 3!)^3 168 \cdot 2$	2,534,400	14	64	319	960	1380
Q_{24}	$d_6^4(b)/aoao/boa^2/oaoa'/oba'a$ $(2^2 \cdot 3!)^4 \cdot 8$	739,200	12	64	327	960	1368
R_{24}	$d_6^2d_8 + 4/b^2o1^4/bob1^20^2/o^2a01^20/ao^201^3/oao1^30$ $(2^2 \cdot 3!)^2 2^3 \cdot 4! \cdot 2$	8,870,400	12	64	327	960	1368
S_{24}	$d_4d_6^3 + 2/abo^21^2/oaob10/aob^20^2/boao01/bo^2a10$ $2 \cdot 2!(2^2 \cdot 3!)^3 \cdot 2$	17,740,800	10	64	335	960	1356
T_{24}	$d_4^4d_8/babab/ba^2oa/oab^2a'/aoba^2/b^2oaa'$ $4^4 \cdot 2^3 \cdot 4! \cdot 8$	4,989,600	10	64	335	960	1356
U_{24}	$d_4^3d_6^2 + 4/ob^2o1^20^2/oa^2o0^31/obob0^21^2/oaoa010^2/b^2o^21^4/a^2o^21010$ $4^2(2^2 \cdot 3!)^2 \cdot 4$	53,222,400	8	64	343	960	1344
V_{24}	$d_4^6(b)/babo^3/obabo^2/o^3babo/o^3bab/bo^3ba/abo^3b$ $4^6 \cdot 6 \cdot 8$	9,979,200	6	64	351	960	1332
W_{24}	$d_4^3d_6 + 6/\ldots$ (see (8.10)) $4^3 \cdot 2^2 \cdot 3! \cdot 3! \cdot 2$	106,444,800	6	64	351	960	1332
X_{24}	$d_4^4 + 8/\ldots$ (see (8.11)) $4^4 \cdot 4! \cdot 2$	159,667,200	4	64	359	960	1320
Y_{24}	$d_4^2 + 16/\ldots$ (see (8.9)) $2^{11} \cdot 3^2$	106,444,800	2	64	367	960	1308
Z_{24}	see (8.13) $2^{10} \cdot 3^3 \cdot 5$	14,192,640	0	64	375	960	1296

words of weight 4 contained in the subcode C') an *extension* of C'. C must contain the vector **1**. So for each C' we must find all its extensions C. Lemma 6.3 is our chief weapon. Having found a C, we compute its group $\mathscr{G}(C)$, and then the number of codes equivalent to C is 24!/order of $\mathscr{G}(C)$. The next two lemmas are typical of the methods used.

LEMMA 8.3. *$C' = d_{24}$ has a unique extension $C = E_{24} = d_{24}/a$* (in the notation of Section 7).

Proof. We must add one vector, u say, to C'. By 6.3 we may assume u is a, b, or a'. But a' is equivalent to a, and b has weight 2, so we may take $u = a$.

LEMMA 8.4. *$C' = d_r (4 \leqslant r \leqslant 22)$ has no extension C.*

Proof. By 6.3, the generator matrix of C has the form

$$\begin{array}{c|c|c} & r & \gamma \\ \hline & d_r & 0 \\ \hline u = & a & \cdots \\ v = & b & \cdots \\ \hline & 0 & Q \end{array},$$

where u and v may be absent. If both are absent C is decomposable. If one is absent, Q has deficiency 0, length $\leqslant 20$, and distance 6, which is impossible by Table III. If both u, v are present, Q has deficiency 1. By Table III there *is* a [20, 9, 6] code Q. But the next lemma shows that this Q, and hence C, does not contain **1**, a contradiction.

Table III, which is frequently used in the proof of Theorem 8.1, shows,

TABLE III

k	1	2	3	4	5	6	7	8	9	10	11	12
n_0	6*	10*	12*	14	15	16*	18	19	20	21	22*	24*

* Code is unique.

for each dimension k, the length n_0 of the shortest s.o. $[n_0, k, 6]$ code. This table was constructed by direct search, with the help of [18]. We omit the details. An asterisk indicates that the code is unique.

LEMMA 8.5. *There is no* s.o. [20, 9, 6] *code containing* **1**.

Proof. Suppose such a code D' exists. By Corollary 3.2 there is a self-dual [20, 10, d] code D containing D'. If $d = 4$, D must be one of the codes E_{20}, K_{20}, L_{20}, M_{20}, R_{20}, S_{20} of [34]. Suppose $D = M_{20}$. Let $v_1, \ldots, v_5$ be the 5 vectors of weight 4 in M_{20}. Then we may assume M_{20} is generated by D' and v_1. Therefore the following vectors are in D': $v_1 + v_2$, $v_1 + v_3$, $v_1 + v_4$, hence $v_1 + v_2 + v_3 + v_4 = \mathbf{1} + v_5$, hence v_5. But v_5 has weight 4, a contradiction. The other possibilities for D, and the case $d = 2$, are similar.

LEMMA 8.6. $d_r d_{24-r}$ (*with* $\gamma = 0$, $\delta = 2$) *has a unique extension* $d_r d_{n-r}/ab/ba$ *provided* $r = 8, 12$.

(This gives the entries A_{24}, H_{24} of Table II.)

LEMMA 8.7. $d_r d_s$ *with* $8 < r + s < 24$ *has no extension.*

One of the most interesting codes in Table II is Y_{24}:

LEMMA 8.8. d_4^2 *has the unique extension* $C = Y_{24}$ *shown in* (8.9).

$Y_{24} =$

1 1 1 1						
	1 1 1 1					
1 1					1 1	1 1 q
1 1				1 1		1 1 r
	1 1				1 1	1 1 s
	1 1			1 1		1 1 t
		1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	u
				1 1 1 1	1 1 1 1	v
			1 1 1 1		1 1 1 1	w
		1 1	1 1	1 1	1 1	x
		1 1	1 1	1 1	1 1	y
		1	1	1	1 1 1	z

(8.9)

Proof. The generator matrix for C must have the form

1 1 1 1 0	0 1 1 1 1	0 0	
a b	0 0	$\cdots$ $\cdots$	q r
0 0	a b	$\cdots$ $\cdots$	s t
0	0	Q	u $\cdots$ z

,

where Q is the unique [16, 6, 6] code mentioned in Table III. To describe Q, let $x_1, \ldots, x_4$ be binary variables. As in describing Reed–Muller codes, we identify each of the 2^{16} polynomials $f(x_1, \ldots, x_4)$ over $GF(2)$ with the corresponding vector of length 16. The first-order Reed–Muller [16, 5, 8] code R consists of all linear function $\sum_{i=1}^{4} \alpha_i x_i + \beta$, where α_i, $\beta = 0$ or 1 [31, Section 5.5]. Then $Q = R \cup (x_1x_2 + x_3x_4 + R)$, so we may take as generators for Q: $u = \mathbf{1}$, $v = x_1$, $w = x_2$, $x = x_3$, $y = x_4$, $z = x_1x_2 + x_3x_4$. The group of R is the general affine group $\mathcal{GA}_4(2)$ consisting of all transformations $(x_1, x_2, x_3, x_4) \to (x_1, x_2, x_3, x_4)A + b$, where A is an invertible 4×4 binary matrix and b is a binary 4-tuple.

It is now straightforward to calculate the group of Q, and to show that there is essentially only one way to choose q, r, s, t, namely $q = x_1x_3$, $r = x_2x_4$, $s = x_1x_4$, $t = x_2x_3$, as shown in (8.9).

The group of Y_{24} is as follows. To every permutation π of the first 4 coordinates there corresponds a permutation $g \in \mathcal{G}(Q)$ such that $\pi \circ g$ fixes Y_{24}. Similarly on the second set of 4. Also the two sets of 4 may be exchanged. Finally there are the 16 permutations generated by $x_i \to x_i + 1$ $(i = 1, \ldots, 4)$. Thus $|\mathcal{G}(Y_{24})| = 24^2 \cdot 2 \cdot 2^4$.

The remaining codes in Table II with minimum distance 4 are found in the same way (although none are as complicated as Y_{24}). It is worth pointing out that d_8^3 has three inequivalent extensions: C_{24}, L_{24}, M_{24}; and d_6^4, d_4^6 each have two.

$d_4^3d_6$ has a unique extension W_{24} shown in (8.10),

W_{24}:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	1	1																				
				1	1	1	1																
								1	1	1	1												
												1	1	1	1								
														1	1	1	1						
												1	1					1	1	1	1	1	1
												1		1		1		1	1	1			
1		1						1	1									1	1		1		1
								1		1								1		1	1		1
1		1		1	1																1		1
				1		1													1	1		1	1
1	1																	1	1		1	1	

(8.10)

and we shall illustrate the general method for finding the group of these codes by calculating $\mathscr{G}(W_{24})$.

The coordinates 1 to 24 of W_{24} are divided naturally into 4 *blocks* (1 2 3 4)(5 6 7 8)(9 10 11 12)(13 14 15 16 17 18) corresponding to the d_4's and the d_6, plus a *gap* (19 ⋯ 24). Candidates for $\mathscr{G}(W_{24})$ fall into 3 classes.

(i) For each d_r block, those permutations in $\mathscr{Z}_2^{(r/2)-1} \cdot \mathscr{S}_r$ which act inside the block, possibly followed by a permutation of the gap (and similarly for each e_7 block, if present). Thus $\mathscr{G}(W_{24})$ contains a Klein 4-group $\mathscr{Z}_2 \cdot \mathscr{S}_2$ acting on each d_4 block, e.g. (13)(24) and (12)(34) fix the code and generate a Klein 4-group on block 1. Again (13 15)(14 16), (13 17)(14 18), (13 14)(15 16), (13 14)(17 18) generate a $\mathscr{Z}_2^2 \cdot \mathscr{S}_3$ on block 4.

(ii) Permutations of the blocks, possibly followed by permutations inside the blocks and inside the gap. Thus in W_{24} a group $\mathscr{S}_3$ acts on blocks 1, 2, 3 as follows. Convention: $\pi \circ \rho$ means first apply π, then ρ. Let π_{12} = (block 1, block 2) = (15)(26)(37)(48), etc. Then

$$\pi_{12} \circ (23)(67)(9\ 11)(19\ 21)(22\ 24),$$
$$\pi_{123} \circ (123)(67)(13\ 14)(19\ 23\ 21\ 22\ 20\ 24)$$

fix the code and generate an $\mathscr{S}_3$ on the blocks.

(iii) Exceptional permutations, not of class (i), which act inside each block, possibly followed by a permutation of the gap. Thus $\mathscr{G}(W_{24})$

contains the exceptional permutation (1 2)(5 7)(9 11)(13 14)(19 22)(20 23)(21 24) of order 2. No other permutations of W_{24} are possible, and the order of $\mathscr{G}(W_{24})$ is $4^3 \cdot (2^2 \cdot 3!) \cdot 3! \cdot 2$.

The only codes containing exceptional permutations are F_{24}, W_{24}, X_{24} (8.11), and Y_{24}.

X_{24}:

1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	
1 1			1 1	1		1
1 1			1 1	1 1	1 1	
	1 1		1 1	1	1	
	1 1	1 1	1 1	1	1	1
	1 1	1 1		1 1	1	1
			1 1	1 1 1 1		

(8.11)

Finally it remains to consider the case of minimum distance 6. Let C be a [24, 12, 6] self-dual code. By deleting 2 coordinates from C we obtain a [22, 11, 4] self-dual code D, which must be in Table I. It is straightforward to show that the only possibility is $D = U_{22}$, and further that there is a unique way to add two columns and one row to the generator matrix of U_{22} to obtain C, as shown in (7.2). Therefore C is unique, and is denoted by Z_{24}.

To simplify calculation of the group of Z_{24}, we give an alternative construction for this code based on the Golay code G_{24}, using the notation of Todd's paper [42].

Let $\Omega = \{\infty, 0, 1, \ldots, 22\}$ be the coordinates of G_{24}. A subset of Ω giving the location of the 1's in a code word of G_{24} of weight 8 is called an *octad*. A list of the 759 octads is given in [42]. Ω may be partitioned into 6 sets of 4 (called *mutually complementary tetrads*) such that the union of any two tetrads is an octad, for example (using Todd's notation for the octads),

$$\infty\ 0\ 1\ 2,\ 3\ 5\ 14\ 17,\ 4\ 13\ 16\ 22,\ 6\ 7\ 19\ 21,\ 9\ 10\ 15\ 20,\ 8\ 11\ 12\ 18. \quad (8.12)$$

Associated with any set of mutually complementary tetrads is a set of 64 *nonspecial hexads* (i.e. 6-sets of Ω) with the properties: (i) A nonspecial

hexad is not contained in any octad; and (ii) let $H = (a_1a_2a_3a_4a_5a_6)$ be any nonspecial hexad, choose any point, say a_1, of H, and find the unique octad $a_2a_3a_4a_5a_6b_2b_3b_4$ containing the other 5 points of H. Then $a_1b_2b_3b_4$ must be one of the tetrads.

A method of constructing the nonspecial hexads is given in [42]. A set of 12 nonspecial hexads associated with the tetrads (8.12) forms the rows of (8.13). These rows do indeed generate a [24, 12, 6] code, which therefore must be Z_{24}. The group of this code is that subgroup of $\mathcal{M}_{24}$ which fixes the set of mutually complementary tetrads. This is the group G_5 described in [42], of order $2^{10} \cdot 3^3 \cdot 5$ and index 1771 in $\mathcal{M}_{24}$. The permutations and character table are given in Table VII of [42]. This completes the proof of Theorem 8.1.

As checks on Table II we verified the formulas of Corollaries 3.3 and 3.12, Section 4, and Theorems 5.3 and 6.8.

Z_{24}:

$$
\begin{array}{c}
\infty\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22 \\
\left[\begin{array}{cccccccccccccccccccccccc}
1 & & & & 1 & 1 & & & 1 & & & 1 & & 1 & & & & & & & & & & \\
 & 1 & & & & & 1 & & & & & & 1 & & & & 1 & & & & 1 & & & 1 \\
 & & 1 & & & & & 1 & & & 1 & & & & 1 & 1 & & & & 1 & & & & \\
 & & & 1 & & & & & & 1 & & & & & & & & 1 & 1 & & & 1 & 1 & \\
 & 1 & & & & & & & & 1 & & & & & 1 & 1 & 1 & & & & & & 1 & \\
 & & 1 & & & & & & & & 1 & & 1 & & & & & 1 & 1 & & 1 & & & \\
 & 1 & & & & & 1 & 1 & & 1 & 1 & & & & & & & 1 & & & & & & \\
 & & 1 & & & & & & & & & & 1 & & & 1 & & & & & & 1 & 1 & 1 \\
 & 1 & & & 1 & & & & & & 1 & & & 1 & 1 & & & & & & 1 & & & \\
 & & 1 & & & 1 & & & & & & & 1 & & & 1 & 1 & & & & 1 & & & \\
 & & 1 & & & 1 & & & 1 & & & & & & & & & & 1 & 1 & & 1 & & \\
 & & & 1 & & 1 & & & & & & 1 & & & & 1 & & & & 1 & & & 1 & \\
\end{array}\right]
\end{array}
$$

(8.13)

Complete Report

Complete versions of Tables I and II covering all [22, 11] and [24, 12] self-dual codes and further details about this work are contained in the 1974 Project MAC Technical Memorandum 49 which is entitled "Complete Classification of [24, 12] and [22, 11] Self-Dual Codes." This report can be obtained from either author.

ACKNOWLEDGMENTS

We thank J. H. Conway for telling us about his enumeration of the self-dual codes of length 24 with weights divisible by 4. In the course of this work we have used the

ALTRAN [5, 17] and MACSYMA [26, 27] programs for algebraic manipulation, and R. Morris's multiple-precision "desk calculator" on the UNIX system [41]. We also wish to thank Richard Fateman for aid in computations.

REFERENCES

1. E. F. ASSMUS, JR., AND H. F. MATTSON, JR., Perfect codes and the Mathieu groups, *Arch. Math.* **17** (1966), 121–135.
2. E. R. BERLEKAMP, "Algebraic Coding Theory," McGraw–Hill, New York, 1968.
3. E. R. BERLEKAMP, Coding theory and the Mathieu groups, *Info. Control* **18** (1971), 40–64.
4. E. R. BERLEKAMP, F. J. MACWILLIAMS, AND N. J. A. SLOANE, Gleason's theorem on self-dual codes, *IEEE Trans. Info. Theory* **18** (1972), 409–414.
5. W. S. BROWN, "ALTRAN User's Manual," 3rd ed., Bell Laboratories, Murray Hill, N. J., 1974.
6. C. C. CADOGAN, The Möbius function and connected graphs, *J. Combinatorial Theory Ser. B* **11** (1971), 193–200.
7. J. H. CONWAY, A perfect group of order 8, 315, 553, 613, 086, 720, 000 and the sporadic simple groups, *Proc. Nat. Acad. Sci. U.S.A.* **61** (1968), 398–400.
8. J. H. CONWAY, A group of order 8, 315, 553, 613, 086, 720, 000, *Bull. London Math. Soc.* **1** (1969), 79–88.
9. J. H. CONWAY, A characterization of Leech's lattice, *Inventiones Math.* **7** (1969), 137–142.
10. J. H. CONWAY, Three lectures on exceptional groups, *in* "Finite Simple Groups," pp.215–247 (M. B. Powell and G. Higman, Eds.), Academic Press, New York, 1971.
11. G. W. FORD AND G. E. UHLENBECK, Combinatorial problems in the theory of graphs, I, *Proc. Nat. Acad. Sci. U.S.A.* **42** (1956), 122–128.
12. E. N. GILBERT, Enumeration of labeled graphs, *Canad. J. Math.* **8** (1956), 405–411.
13. A. M. GLEASON, Weight polynomials of self-dual codes and the MacWilliams identities, *in* "Actes Congr. Inter. Math., Nice 1970," Vol. 3, pp. 211–215, Gauthier–Villars, Paris, 1970.
14. J. M. GOETHALS, F. J. MACWILLIAMS, AND C. L. MALLOWS, Further remarks on extremal self-dual codes, to appear.
15. M. J. E. GOLAY, Notes on digital coding, *Proc. IEEE* **37** (1949), 657.
16. M. J. E. GOLAY, Binary coding, *IEEE Trans. Info. Theory* **4** (1954), 23–28.
17. A. D. HALL, JR., The ALTRAN system for rational function manipulation—a survey, *Commun. Assoc. Computing Machinery* **14** (1971), 517–521.
18. H. J. HELGERT AND R. D. STINAFF, Minimum-distance bounds for binary linear codes, *IEEE Trans. Info. Theory* **19** (1973), 344–356.
19. M. KARLIN, New binary coding results by circulants, *IEEE Trans. Info. Theory* **15** (1969), 81–92.
20. M. G. KENDALL AND A. STUART, "The Advanced Theory of Statistics," Vol. 1., pp. 155–156, Hafner, New York, 1969.
21. J. LEECH, Some sphere packings in higher space, *Canad. J. Math.* **16** (1964), 657–682.
22. J. LEECH AND N. J. A. SLOANE, Sphere packings and error-connecting codes, *Canad. J. Math.* **23** (1971), 718–745.

23. F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Info. Theory* **18** (1972), 794–805.
24. F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, Good self dual codes exist, *Discrete Math.* **3** (1972), 153–162.
25. C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, *Info. Control* **22** (1973), 188–200.
26. W. A. Martin and R. J. Fateman, The MACSYMA system, *in* "Proc. Second A.C.M. Symposium on Symbolic and Algebraic Manipulation, Los Angeles, California, March 1971."
27. Mathlab Group, Project MAC, "MACSYMA Reference Manual," version 5, Massachusetts Institute of Technology, Cambridge, Mass., 1973.
28. J. Milnor and D. Husemoller, "Symmetric Bilinear Forms," Appendix 4, Springer–Verlag, Berlin, 1973.
29. H. V. Niemeier, Definite quadratische Formen der Dimension 24 und Diskriminante 1, *J. Number Theory* **5** (1973), 142–178.
30. L. J. Paige, A Note on the Mathieu groups, *Canad. J. Math.* **9** (1957), 15–18.
31. W. W. Peterson and E. J. Weldon, Jr., "Error-Connecting Codes," 2nd Ed., MIT Press, Cambridge, Mass., 1972.
32. Vera Pless, The number of isotropic subspaces in a finite geometry, *Accad. Naz. Lincei., Rend. Cl. Sci. Fiz., Mat. e Nat. (8)* **39** (1965), 418–421.
33. Vera Pless, On the uniqueness of the Golay codes, *J. Combinatorial Theory* **5** (1968), 215–228.
34. Vera Pless, A classification of self-orthogonal codes over $GF(2)$, *Discrete Math.* **3** (1972), 209–246.
35. Vera Pless and J. N. Pierce, Self-dual codes over $GF(q)$ satisfy a modified Varshamov bound, *Information and Control* **23** (1973), 35–40.
36. John Riordan, "An Introduction to Combinatorial Analysis," Wiley, New York, 1958.
37. John Riordan, "Combinatorial Identities," Wiley, New York, 1968.
38. D. Slepian, Some further theory of group codes, *Bell Syst. Tech. J.* **39** (1960), 1219–1252. (Reprinted in "Algebraic Coding Theory: History and Development" [I. F. Blake, Ed.], Dowden, Hutchinson and Ross, Stroudsberg, PA., 1973.)
39. S. L. Snover, The uniqueness of the Nordstrom–Robinson and Golay binary codes, Ph.D. dissertation, Michigan State University, East Lansing, Mich., 1973.
40. R. Stanton, The Mathieu groups, *Canad. J. Math.* **3** (1951), 164–174.
41. K. Thompson and D. M. Ritchie, "UNIX Programmer's Manual," 2nd Ed., Bell Laboratories, Murray Hill, N.J., 1972.
42. J. A. Todd, A representation of the Mathieu group M_{24} as a collineation group, *Ann. di Math. Pura ed Appl., (IV)* **71** (1966), 199–238.
43. E. Witt, Über Steinersche Systeme, *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 265–275.